PTO/SB/21 (08-03)
Approved for use through 08/30/2003. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/712,869
Filing Date	11/12/03
First Named Inventor	Keiichi Iwamura
Art Unit	2131
Examiner Name	
Total Number of Pages in This Submission: 74	Attorney Docket Number: CFA00018US

ENCLOSURES *(Check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment/Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☑ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance communication to Technology Center (TC)
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Other Enclosure(s) (please Identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Canon U.S.A., Inc. IP Department Fidel Nwamu
Signature	
Date	3/1/04

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Typed or printed name	Fidel Nwamu		
Signature		Date	3/1/04

CFA 00018
US

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１０月　３日

出願番号
Application Number: 特願２００３－３４６１４０

[ST. 10/C]: [ＪＰ２００３－３４６１４０]

出願人
Applicant(s): キヤノン株式会社

２００３年１２月　２日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３０９９３８０

【書類名】　特許願
【整理番号】　256811
【提出日】　平成15年10月 3日
【あて先】　特許庁長官殿
【国際特許分類】　H04N 5/00
【発明者】
　【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
　【氏名】　岩村　恵市
【特許出願人】
　【識別番号】　000001007
　【氏名又は名称】　キヤノン株式会社
【代理人】
　【識別番号】　100090273
　【弁理士】
　【氏名又は名称】　國分　孝悦
　【電話番号】　03-3590-8901
【先の出願に基づく優先権主張】
　【出願番号】　特願2002-332577
　【出願日】　平成14年11月15日
【手数料の表示】
　【予納台帳番号】　035493
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9705348

【書類名】特許請求の範囲
【請求項１】
所定の作者により作成された原データを処理する情報処理装置であって、
前記原データを変更する際に、その変更に関する変更情報を保持する保持手段と、
前記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成手段とを有することを特徴とする情報処理装置。
【請求項２】
前記変更情報を正当なものとするかを判定する判定手段をさらに有し、
前記判定手段で正当なものとすると判定された場合に、前記変更保証情報作成手段は、前記変更保証情報を作成することを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記原データが原本であることを保証するための原データ保証情報を保持する原データ保証情報保持手段をさらに有することを特徴とする請求項１または２に記載の情報処理装置。
【請求項４】
前記原データを変更処理する変更処理手段をさらに有することを特徴とする請求項１～３の何れか１項に記載の情報処理装置。
【請求項５】
前記変更保証情報と、前記原データ保証情報は、デジタル署名であることを特徴とする請求項３または４に記載の情報処理装置。
【請求項６】
前記変更情報は、前記原データを特定する情報と、前記変更処理手段を特定する情報と、前記原データを変更する際に行った変更処理を特定する情報とを含むことを特徴とする請求項４または５に記載の情報処理装置。
【請求項７】
前記変更情報は、前記原データと、前記原データに対する変更データとの差分情報を含むことを特徴とする請求項１～５の何れか１項に記載の情報処理装置。
【請求項８】
前記判定手段は、設定されたアクセス権限を用いて判定することを特徴とする請求項２～７の何れか１項に記載の情報処理装置。
【請求項９】
前記判定手段は、前記原データの作者の公開鍵を用いて判定することを特徴とする請求項２～７の何れか１項に記載の情報処理装置。
【請求項１０】
前記原データと、前記原データ保証情報と、前記変更情報と、前記変更保証情報とを管理する管理手段をさらに有することを特徴とする請求項３～９の何れか１項に記載の情報処理装置。
【請求項１１】
前記原データと、前記原データ保証情報と、前記変更情報と、前記変更保証情報とを送付する送付手段をさらに有することを特徴とする請求項３～９の何れか１項に記載の情報処理装置。
【請求項１２】
所定の作者により作成された原データを処理する情報処理装置であって、
前記原データが原本として保証されたものであることを確認する原データ確認手段と、
前記原データの変更に関する変更情報が原本として保証されたものであることを確認する変更情報確認手段と、
前記原データと前記変更情報が原本として保証されたものであることが確認された場合に、前記変更情報に応じて前記原データを変更する変更手段とを有することを特徴とする情報処理装置。
【請求項１３】

前記原データ確認手段は、前記原データに対するデジタル署名を検証し、前記変更情報確認手段は、前記変更情報に対するデジタル署名を検証するようにしたことを特徴とする請求項１２に記載の情報処理装置。

【請求項１４】

前記請求項３～９の何れか１項に記載の情報処理装置とネットワークで接続されたサーバ装置であって、

前記原データと、前記原データ保証情報と、前記変更情報と、前記変更保証情報とを、前記情報処理装置より受信し、管理することを特徴とするサーバ装置。

【請求項１５】

ネットワークに接続された情報処理装置を複数有する電子データ管理システムであって、

前記情報処理装置は、前記ネットワーク上で共有された電子データが原本として保証されたものであることと、前記電子データの変更に関する第１の変更情報が原本として保証されたものであることとを確認する確認手段と、

前記電子データと前記第１の変更情報が、前記確認手段により原本として保証されたものであることが確認された場合に、前記電子データを変更する電子データ変更手段と、

前記電子データ変更手段により変更された電子データの変更に関する第２の変更情報と、前記第２の変更情報が原本であることを保証するための変更保証情報とを作成する情報作成手段と、

前記情報作成手段により作成された第２の変更情報と、変更保証情報とを前記ネットワークに送信する送信手段とを有し、

前記複数の情報処理装置で共同して前記電子データの管理を行うようにしたことを特徴とする電子データ管理システム。

【請求項１６】

第１の情報処理装置と、前記第１の情報処理装置とネットワークを介して接続された第２の情報処理装置とを有する情報処理システムであって、

前記第１の情報処理装置は、前記第１の情報処理装置から電子データを受信する手段と、

前記受信した電子データを変更し、その変更に関する変更情報と、前記変更情報が原本であることを保証するための第１の変更保証情報とを作成する手段と、

前記変更情報と前記第１の変更保証情報を、前記第２の情報処理装置に送信する手段とを有し、

前記第２の情報処理装置は、前記第１の情報処理装置により送信された変更情報が原本として保証されたものであることを、前記第１の変更保証情報を用いて確認する手段と、

前記変更情報を正当なものとするかを判定する手段と、

前記判定手段で正当なものとすると判定された場合に、前記変更情報が原本であることを保証するための第２の変更保証情報を作成する手段と、

前記第２の変更保証情報を、前記第１の情報処理装置に送信する手段とを有することを特徴とする情報処理システム。

【請求項１７】

所定の作者により作成された原データを処理する情報処理方法であって、

前記原データを変更する際に、その変更に関する変更情報を保持する保持工程と、

前記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成工程とを行うことを特徴とする情報処理方法。

【請求項１８】

前記変更情報を正当なものとするかを判定する判定工程をさらに有し、

前記判定工程で正当なものとすると判定された場合に、前記変更保証情報作成工程は、前記変更保証情報を作成することを特徴とする請求項１７に記載の情報処理方法。

【請求項１９】

所定の作者により作成された原データを処理する情報処理方法であって、

前記原データが原本として保証されたものであることを確認する原データ確認工程と、
前記原データの変更に関する変更情報が原本として保証されたものであることを確認する変更情報確認工程と、
前記原データと前記変更情報が原本として保証されたものであることが確認された場合に、前記変更情報に応じて前記原データを変更する変更工程とを行うことを特徴とする情報処理方法。

【請求項２０】
前記原データ確認工程は、前記原データに対するデジタル署名を検証し、前記変更情報確認処理は、前記変更情報に対するデジタル署名を検証するようにしたことを特徴とする請求項１９に記載の情報処理方法。

【請求項２１】
前記請求項１７～２０の何れか１項に記載の情報処理方法をコンピュータに実行させることを特徴とするコンピュータプログラム。

【請求項２２】
前記請求項２１に記載のコンピュータプログラムを記憶することを特徴とするコンピュータ読み取り可能な記憶媒体。

【書類名】明細書
【発明の名称】情報処理装置、サーバ装置、電子データ管理システム、情報処理システム、情報処理方法、コンピュータプログラム及びコンピュータ読み取り可能な記憶媒体
【技術分野】
【０００１】
本発明は、情報処理装置、サーバ装置、電子データ管理システム、情報処理システム、情報処理方法、コンピュータプログラム及びコンピュータ読み取り可能な記憶媒体に関し、特に、データの原本性を保証するために用いて好適なものである。
【背景技術】
【０００２】
近年、コンピュータやインターネットの普及に伴い、情報をデジタル化し、デジタルデータとして利用する形態が一般化しつつある。一方、デジタルデータでは、まったく同質なコピーを容易に生成でき、編集処理も容易に実行できるという特徴がある。そのため、デジタルデータの原本性を保証することは重要である。
【０００３】
一般に、デジタルデータの原本性を保証するには、例えば、米国特許第５４９９２９４号明細書（特許文献１）に示されているように、デジタル画像のハッシュ値に公開鍵暗号を用いた電子署名を作成することによって実現できることが知られている。米国特許第５４９９２９４号明細書では、電子署名データを生成するために、ハッシュ関数と公開鍵暗号とを使用している。上記電子署名とは、送信者がデータと一緒に該データに対応する署名データを送り、受信者がその署名データを検証して該データの正当性を確認することができるようにするものである。
【０００４】
ハッシュ関数と公開鍵暗号とを用いて電子署名データを生成してデータの正当性を確認する方法は、具体的に以下のようである。ここでは、米国特許第５４９９２９４号明細書に記載されている方法に、公知技術として知られている技術を付け加えて、わかりやすく説明する。
まず、秘密鍵をＫｓ、公開鍵をＫｐとすると、送信者は、平文データＭをハッシュ関数により圧縮して一定長の出力ｈを算出する演算を行う（一定長の出力ｈは、ハッシュ値と呼ばれる。）。
次に、秘密鍵Ｋｓで一定長の出力ｈを変換して電子署名データｓを作成する演算を行う。この演算を以下の（１式）のように表現する。
Ｄ(Ks, h)＝ｓ・・・（１式）
その後、該電子署名データｓと平文データＭとを受信者に送信する。
【０００５】
一方、受信者は、受信した電子署名データｓを公開鍵Ｋｐで変換する演算を行う。この演算を以下の（２式）のように表現する。
Ｅ(Kp, s)＝Ｅ(Kp, Ｄ(Ks, h''))＝h'' ・・・（２式）
また、受信者は、受信した平文データM'を送信者と同じハッシュ関数により圧縮して一定長の出力ｈ'を算出する演算を行う。そして、この演算で算出された一定長の出力ｈ'と、上記（２式）により得られた一定長の出力ｈ''とが一致すれば、受信した平文データM'が正当であると判断する。
【０００６】
平文データＭが送受信間で改ざんされた場合には、上記（２式）により得られた一定長の出力ｈ''と、受信した平文データM'を発信者と同じハッシュ関数により圧縮して得られた一定長の出力ｈ'とが一致しないので改ざんを検出できる。
ここで、平文データＭの改ざんに合わせて電子署名データｓの改ざんも行われてしまうと改ざんを検出することができなくなる。しかし、電子署名データｓを改ざんするには、一定長の出力ｈから平文データＭを求める必要があるが、このような計算はハッシュ関数の一方向性により不可能である。

次に、ハッシュ関数について説明する。

【０００７】

ハッシュ関数は、電子署名データｓの生成を高速化するため等に用いられる。ハッシュ関数は、任意の長さの平文データＭを処理して、一定の長さの出力（一定長の出力）ｈを出す機能を持つ。ここで、一定長の出力ｈを平文データＭのハッシュ値（またはメッセージダイジェスト、デジタル指紋）という。

ハッシュ関数に要求される性質として、一方向性と衝突耐性がある。一方向性とは、一定長の出力ｈを与えた時に、ｈ＝Ｈ（Ｍ）となる平文データＭの算出が計算量的に困難であることである。衝突耐性とは、平文データＭを与えた時に、Ｈ（Ｍ）＝Ｈ（Ｍ'）となる平文データＭ'（Ｍ≠Ｍ'）を算出することが計算量的に困難であること、及びＨ（Ｍ）＝Ｈ（Ｍ'）かつＭ≠Ｍ'となる平文データＭ，Ｍ'を算出することが計算量的に困難であることである。

ハッシュ関数としては、MD-2、MD-4、MD-5、SHA-1、RIPEMD-128、及びRIPEMD-160等が知られており、これらのアルゴリズムは、一般に公開されている。

【０００８】

次に、公開鍵暗号について説明する。

公開鍵暗号は、暗号鍵と復号鍵が異なり、暗号鍵を公開し、復号鍵を秘密に保持する暗号方式である。公開鍵暗号の主な特徴として、以下の３つのことが挙げられる。

（ａ）暗号鍵と復号鍵とが異なり暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

（ｂ）各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみを秘密に記憶しておけばよい。

（ｃ）送られてきた通信文の送信者が偽者でないこと、及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。

【０００９】

例えば、平文データＭに対して、公開の暗号鍵Ｋｐを用いた暗号化操作をＥ(Kp,M)とし、秘密の復号鍵Ｋｓを用いた復号化操作をＤ(Ks,M)とすると、公開鍵暗号アルゴリズムは、次の２つの条件を満たす。

（１）公開の暗号鍵Ｋｐが与えられたとき、暗号化操作Ｅ(Kp,M)の計算は容易である。秘密の復号鍵Ｋｓが与えられたとき、復号化操作Ｄ(Ks,M)の計算は容易である。

（２）もし、秘密の復号鍵Ｋｓを知らないのなら、公開の暗号鍵Ｋｐと、暗号化操作Ｅの計算手順と、Ｃ＝Ｅ(Kp,M)を知っていても、平文データＭを決定することは計算量の点で困難である。

次に、上記（１）、（２）の条件に加えて、次の（３）の条件が成立することにより、秘密通信を実現できる。

（３）全ての平文データＭに対し、暗号化操作Ｅ(Kp,M)を定義でき、以下の（４式）が成立する。

Ｄ(Ks,Ｅ(Kp,M))＝Ｍ・・・（４式）

つまり、公開の暗号鍵Ｋｐは公開されているため、誰もが暗号化操作Ｅ(Kp,M)を計算することができるが、復号化操作Ｄ(Ks,Ｅ(Kp,M))を計算して平文データＭを得ることができるのは秘密の復号鍵Ｋｓを持っている本人だけである。

【００１０】

一方、上記（１）、（２）の条件に加えて、次の（４）の条件が成立することにより認証通信を実現できる。

（４）すべての平文データＭに対し、復号化操作Ｄ(Ks,M)を定義でき、以下の（５式）が成立する。

Ｅ(Kp,Ｄ(Ks,M))＝Ｍ・・・（５式）

つまり、復号化操作Ｄ(Ks,M)を計算できるのは、秘密の復号鍵Ｋｓを持っている本人のみであり、他の人が偽の秘密の復号鍵Ｋｓ'を用いて復号化操作Ｄ(Ks',M)を計算し、秘密の復号鍵Ｋｓを持っている本人になりすましたとしても、上記（５式）が成立しない

ので（E(Kp, D(Ks', M))≠M）、受信者は、受けとった情報が不正なものであることを確認できる。

【００１１】

また、復号化操作D(Ks, M)が改ざんされても上記（５式）が成立しなくなり（E(Kp, D(Ks, M)')≠M）、受信者は、受けとった情報が不正なものであることを確認できる。

上記の秘密通信と認証通信とを行うことができる代表例として、RSA暗号やR暗号やW暗号等が知られている。

ここで、現在最も使用されている上記RSA暗号による暗号化と復号は、以下の（６式）で示される。

暗号化：暗号化鍵（e, n）　暗号化変換C=Me(mod n)

復号：復号鍵（d, n）　復号変換M=Cd(mod n)

n=p・q

ここで、p、qは、大きな異なる素数・・・（６式）

このように、米国特許第５４９９２９４号明細書には、デジタル画像のハッシュ値に公開鍵暗号を用いた電子署名を作成し、デジタルデータの原本性を保証することが記載されている。

【００１２】

【特許文献１】米国特許第５４９９２９４号明細書

【発明の開示】

【発明が解決しようとする課題】

【００１３】

しかしながら、米国特許第５４９９２９４号明細書に記載されている手法では、電子署名をつけたデジタルデータを１ビットでも変更した場合、著者が認めた正当な変更であっても、改ざんとして検出される。さらに、米国特許第５４９９２９４号明細書に記載されている手法では、データを変更した後に関しては、その変更したデータが原本でないことだけが分かるだけである。

【００１４】

例えば、米国特許第５４９９２９４号明細書をデジタルカメラに適用した例を考える。通常、デジタルカメラからの出力であるデジタル画像と電子署名データは、コンピュータ（PC）に取り込まれる。その後、画像が見やすいように輝度を変更したり、フィルタリングをしたり、または画像を小さくするために余計な部分を切り取ったりすることは通常よく行われる。

これらの処理は、画像を見やすく、分かりやすくするための処理であり、デジタル画像の著作者が認めている処理である場合が多い。しかしながら、米国特許第５４９９２９４号明細書に記載されている技術では、デジタルカメラから出力された後に行われた全ての処理は改ざんとして検出される。

このように従来の技術では、電子署名などによりデータの原本性が保証されているような場合には、上記データを正当なデータとして変更することができないという問題点があった。

【００１５】

本発明は上述の問題点に鑑みてなされたものであり、データの原本性を保証しながら、上記データの作者が認める正当な変更を行えるようにすることを目的とする。

【課題を解決するための手段】

【００１６】

本発明の情報処理装置は、所定の作者により作成された原データを処理する情報処理装置であって、前記原データを変更する際に、その変更に関する変更情報を保持する保持手段と、前記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成手段とを有することを特徴とする。

また、本発明の他の特徴とするところは、所定の作者により作成された原データを処理する情報処理装置であって、前記原データが原本として保証されたものであることを確認

する原データ確認手段と、前記原データの変更に関する変更情報が原本として保証されたものであることを確認する変更情報確認手段と、前記原データと前記変更情報が原本として保証されたものであることが確認された場合に、前記変更情報に応じて前記原データを変更する変更手段とを有することにある。

本発明のサーバ装置は、前記何れかに記載の情報処理装置とネットワークで接続されたサーバ装置であって、前記原データと、前記原データ保証情報と、前記変更情報と、前記変更保証情報とを、前記情報処理装置より受信し、管理することを特徴とする。

本発明の電子データ管理システムは、ネットワークに接続された情報処理装置を複数有する電子データ管理システムであって、前記情報処理装置は、前記ネットワーク上で共有された電子データが原本として保証されたものであることと、前記電子データの変更に関する第１の変更情報が原本として保証されたものであることとを確認する確認手段と、前記電子データと前記第１の変更情報が、前記確認手段により原本として保証されたものであることが確認された場合に、前記電子データを変更する電子データ変更手段と、前記電子データ変更手段により変更された電子データの変更に関する第２の変更情報と、前記第２の変更情報が原本であることを保証するための変更保証情報とを作成する情報作成手段と、前記情報作成手段により作成された第２の変更情報と、変更保証情報とを前記ネットワークに送信する送信手段とを有し、前記複数の情報処理装置で共同して前記電子データの管理を行うようにしたことを特徴とする。

本発明の情報処理システムは、第１の情報処理装置と、前記第１の情報処理装置とネットワークを介して接続された第２の情報処理装置とを有する情報処理システムであって、前記第１の情報処理装置は、前記第１の情報処理装置から電子データを受信する手段と、前記受信した電子データを変更し、その変更に関する変更情報と、前記変更情報が原本であることを保証するための第１の変更保証情報とを作成する手段と、前記変更情報と前記第１の変更保証情報を、前記第２の情報処理装置に送信する手段とを有し、前記第２の情報処理装置は、前記第１の情報処理装置により送信された変更情報が原本として保証されたものであることを、前記第１の変更保証情報を用いて確認する手段と、前記変更情報を正当なものとするかを判定する手段と、前記判定手段で正当なものとすると判定された場合に、前記変更情報が原本であることを保証するための第２の変更保証情報を作成する手段と、前記第２の変更保証情報を、前記第１の情報処理装置に送信する手段とを有することを特徴とする。

【００１７】

本発明の情報処理方法は、所定の作者により作成された原データを処理する情報処理方法であって、前記原データを変更する際に、その変更に関する変更情報を保持する保持工程と、前記変更情報が原本であることを保証するための変更保証情報を作成する変更保証情報作成工程とを行うことを特徴とする。

また、本発明の他の特徴とするところは、所定の作者により作成された原データを処理する情報処理方法であって、前記原データが原本として保証されたものであることを確認する原データ確認工程と、前記原データの変更に関する変更情報が原本として保証されたものであることを確認する変更情報確認工程と、前記原データと前記変更情報が原本として保証されたものであることが確認された場合に、前記変更情報に応じて前記原データを変更する変更工程とを行うことにある。

【００１８】

本発明のコンピュータプログラムは、前記何れかに記載の情報処理方法をコンピュータに実行させることを特徴とする。

本発明のコンピュータ読み取り可能な記憶媒体は、前記記載のコンピュータプログラムを記憶することを特徴とする。

【発明の効果】

【００１９】

本発明によれば、所定の作者により作成された原データを変更する際に、その変更に関する変更情報を保持するとともに、前記変更情報が原本であることを保証するための変更

保証情報を作成するようにしたので、前記変更保証情報に基づいて前記原データの変更が正当なものであるか否かを判断し、正当なものである場合には前記変更情報により前記原データを変更することができるようになる。したがって、前記原データの原本性を保証しながら、前記原データの作者が認める正当な変更を行うことができ、前記原データの原本性と、データの最新性の両方を保証することができる。また、前記変更情報により、前記原データと、変更したデータとの関係を知ることができ、前記原データと、変更したデータとが適切な関係にあることを保証することができる。さらに、前記変更情報は、前記変更したデータそのものに比べてデータ量が少ないので、前記原データを変更するのに要する記憶容量を可及的に小さくすることができる。

【発明を実施するための最良の形態】

【００２０】

以下、本発明の実施形態について、図面を参照して詳細に説明する。なお、ここではオリジナルのデジタルデータを原画像と呼ぶが、本実施の形態で適用されるデジタルデータ（原データ）は、デジタル画像だけに限らず、デジタルデータ全てに適用できる。

（第１の実施の形態）

本発明の第１の実施の形態を、図面を参照しながら説明する。

まず、原画像に対する電子署名を生成する。これは、前述した米国特許第５４９９２９４号明細書ように、原画像に対するハッシュ値を生成し、そのハッシュ値に対して秘密鍵で電子署名を作成することによって実現できる。この電子署名を第１の署名（図１の署名０）１１と表し、図１（ａ）に示されるように原画像１２とともに保存する。

【００２１】

次に、保存された原画像１２に対して第１の処理を施して、その処理結果を正当な画像として認める場合を考える。ここで、第１の処理とは、画像が見やすいように輝度を変更したり、フィルタリングをしたり、または画像を小さくするために余計な部分を切り取ったりすることなど、原画像に変更を加える処理である。上述した電子署名の原理は、デジタルデータ全てに利用でき、ここでも、上述した電子署名の原理を用いて、履歴情報１３に対する電子署名を作成する。つまり、履歴情報１３に対するハッシュ値を生成し、そのハッシュ値に対して秘密鍵で電子署名を作成する。

【００２２】

ここで、履歴情報１３とは、上記第１の処理で行われた原画像１２の変更（履歴）に関する情報である。なお、以下の説明では、この履歴情報１３に対する電子署名を第２の署名（図１の署名１）１４と称する。

例えば、上記第1の処理が、PhotoShop ver.Xというエディタで行った輝度変換である場合、上記第１の処理に対する履歴情報１３は、対象画像を特定する情報と、上記エディタを特定する情報と、上記エディタで規定されている輝度変換というフィルタ名と、それに用いたパラメータ情報などから構成される。

また、履歴情報１３は、原画像１２と変更画像との差分データを含んでいても良い。ここで、対象画像を特定する情報は、原画像１２のID番号や、原画像１２に対する署名である第１の署名（図１の署名０）などを用いることができる。そして、このようにして作成された履歴情報１３と第２の署名１４とを図１（ｂ）に示されるように原画像１２と一緒に保存する。

【００２３】

上記の処理は、著作者によって行われる処理である。次に、上記第１の処理により輝度変換された画像の入手を他のユーザが希望している場合を考える。著作者は、図１（ｂ）のように、記憶媒体に保存されている原画像１２、第１の署名（図１の署名０）１１、履歴情報１３、及び第２の署名（図１の署名１）１４を、通信手段を用いてそのユーザに送信する。

【００２４】

以下、これらの情報が送られたユーザが行う検証処理について説明する。

まず、原画像１２に対する第１の署名（図１の署名０）１１を確認する。原画像１２の

著作者の公開鍵を用いて、第１の署名（図１の署名０）１１を変換して出力ｈを得るとともに、原画像１２のハッシュ値ｈ'を得て、出力ｈとハッシュ値ｈ'とが同じであるかを見ることで、第１の署名（図１の署名０）１１の確認を行う。

【００２５】

次に、履歴情報１３に対する第２の署名（図１の署名１）１４を確認する。履歴情報１３の著作者の公開鍵を用いて、第２の署名（図１の署名１）１４を変換して出力ｈを得るとともに、履歴情報１３のハッシュ値ｈ'を得て、出力ｈとハッシュ値ｈ'とが同じであるかを見ることで、第２の署名（図１の署名１）１４の確認を行う。

原画像１２と履歴情報１３の正当性が第１の署名１１と第２の署名１４により確認された後、履歴情報１３に書かれた情報に基づいて、上記第１の処理と同じ処理を、原画像１２に対して行うことにより、ユーザは、輝度変換された画像を得ることができる。

【００２６】

図２は、以上のような処理を行う本実施形態の情報処理装置の構成の一例を示したブロック図である。なお、本発明の情報処理装置の実現に当たっては、図２に示される全ての機能を使用することは必須ではない。

図２において、情報処理装置（コンピュータ）３０１のハードウェアは、一般に普及しているパーソナルコンピュータであり、スキャナ等の画像入力装置３１７から読み取られた画像を入力し、編集や保管を行うことが可能である。

また、画像入力装置３１７で得られた画像をプリンタ３１６から印刷させることができる。なお、ユーザからの各種指示等は、マウス３１３やキーボード３１４などからの入力操作により行われる。

【００２７】

コンピュータ３０１の内部では、バス３０７により後述する各ブロックが接続され、種々のデータの受け渡しが可能である。図２において、ＭＰＵ３０２は、コンピュータ３０１内部の各ブロックの動作を制御し、あるいは内部に記憶されたプログラムを実行することができる。

主記憶装置３０３は、ＭＰＵ３０２において行われる処理のために、一時的にプログラムや処理対象の画像データを格納しておく装置である。ハードディスク（ＨＤＤ）３０４は、主記憶装置３０３等に転送されるプログラムや画像データをあらかじめ格納したり、処理後の画像データを保存したりすることのできる装置である。

【００２８】

スキャナインタフェース（Ｉ／Ｆ）３１５は、原稿やフィルム等を読み取って、画像データを生成するスキャナ３１７と接続され、スキャナ３１７で得られた画像データを入力することのできるインターフェース（Ｉ／Ｆ）である。

プリンタインタフェース３０８は、画像データを印刷するプリンタ３１６と接続され、印刷する画像データをプリンタ３１６に送信することのできるインターフェース（Ｉ／Ｆ）である。

【００２９】

ＣＤドライブ（ＣＤ）３０９は、外部記憶媒体の一つであるＣＤ（ＣＤ－Ｒ／ＣＤ－ＲＷ）に記憶されたデータを読み出したり、あるいは書き込んだりすることができる装置である。

ＦＤＤドライブ（ＦＤＤ）３１１は、ＣＤドライブ３０９と同様に、外部記憶装置の一つであるＦＤＤ（フレキシブルディスク）からの読み出しや、ＦＤＤへの書き込みをすることができる装置である。

ＤＶＤドライブ（ＤＶＤ）３１０は、ＦＤＤドライブ３１１と同様に、外部記憶装置の一つであるＤＶＤからの読み出しや、ＤＶＤへの書き込みをすることができる装置である。

【００３０】

なお、ＣＤ、ＦＤＤ、ＤＶＤ等に画像編集用のプログラム、あるいはプリンタドライバが記憶されている場合には、これらプログラムをハードディスク（ＨＤＤ）３０４上にイ

ンストールし、必要に応じて主記憶装置３０３に転送されるようになっている。
インターフェース（Ｉ／Ｆ）３１２は、マウス３１３やキーボード３１４からの入力指示を受け付けるために、これらと接続されるインターフェース（Ｉ／Ｆ）である。
また、モニタ３０６は、透かし情報の抽出処理結果や処理過程を表示することのできる表示装置である。さらに、ビデオコントローラ３０５は、表示データをモニタ３０６に送信するための装置である。
なお、本実施の形態では、情報処理装置３０１に上述した機能を全て搭載するようにしたが、上述した機能を分配して複数の装置からなるシステムとしてもよい。すなわち、複数の機器（例えば、ホストコンピュータ、インターフェース機器、リーダ、プリンタ等）から構成されるシステムにしても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置等）にしてもよい。
【００３１】
次に、図３と図４を参照しながら、本実施の形態の情報処理装置３０１の動作について説明する。図３は、電子署名を生成する際の情報処理装置３０１の処理を説明するフローチャートである。また、図４は、電子署名を検証する際の情報処理装置３０１の処理を説明するフローチャートである。
なお、原画像１２に対する第１の署名（図１の署名０）１１を生成する際の処理は、上述した米国特許第５４９９２９４号明細書に記載されている技術と同様にして行えるので説明を省略し、ここでは、原画像１２と第１の署名（図１の署名０）１１が、情報処理装置３０１内の記憶媒体に保存されているという前提で説明する。
【００３２】
まず、図３に示す電子署名（第２の署名（図１の署名１）１４）を生成する際の処理を説明する。なお、以下では必要に応じてこの処理を署名生成処理と称する。
記憶媒体に保存された原画像１２を入力する（ステップＳ２０１）。これは、ハードディスク（ＨＤＤ）３０４、ＣＤドライブ（ＣＤ）３０９、ＤＶＤドライブ（ＤＶＤ）３１０、またはＦＤＤドライブ（ＦＤＤ）３１１などに接続された各記憶媒体に格納されている原画像１２を、マウス３１３やキーボード３１４からの入力指示により、主記憶装置３０３にロードすることにより実現される。
【００３３】
次に、その原画像１２に対して変更処理を行う（ステップＳ２０２）。このときに行った変更処理に関する履歴情報１３を記憶媒体に記憶する（ステップＳ２０３）。なお、この変更処理は、複数の処理を組み合わせても良い。
変更処理が正当な処理かを判断する（ステップＳ２０４）。
【００３４】
ここで、全ユーザのアクセス権限が保存されている不図示のアクセス権限データベースに、そのユーザのアクセス権限が設定されている。そして、上記変更処理の正当性の検証は、図２に示すコンピュータへのログイン時に得られる認証情報を基に、上記アクセス権限の範囲内の変更であれば正当と判断する一方、その範囲を超えていれば正当でないと判断することによりなされる。この他、原画像１２の内部やヘッダなどにアクセスに関する許諾範囲を著作者により記述するようにし、それを、変更処理を行うエディタが読み込んで、許諾範囲内の変更であれば正当と判断する一方、許諾範囲を超えていれば正当でないと判断することによっても、上記変更処理の正当性の検証はなされる。
【００３５】
また、上記変更処理の正当性の検証を、公開鍵を用いることによっても行うことが可能である。原画像１２に対する第１の署名（署名０）１１の正当性を見る際には、原画像１２の著作者の公開鍵を用いるが、履歴情報１３に対する第２の署名（署名１）１４の正当性を見る際にも、先ほど用いた原画像１２の著作者の公開鍵を用いて検証することによって、原画像１２の著作者が変更処理を行ったか否かがわかる。
【００３６】
そして、これらの処理は、マウス３１３やキーボード３１４からの入力指示に応じて主

記憶装置３０３にロードしたプログラムを、ＭＰＵ３０２などを用いて実行することにより行われる。このとき、モニタ３０６により実行状況や、その結果をモニタすることも可能である。

このように変更処理の正当性の検証を行い、変更処理した画像が正当であると認められない場合には、処理結果及び処理履歴を廃棄し、前の画像（原画像１２）に戻す。また、変更処理された画像を正当な画像として認める場合、記憶媒体に記憶された履歴情報１３に対して電子署名（第２の署名（図１の署名１）１４）を作成する（ステップＳ２０５）。生成した原画像１２、第１の署名（図１の署名０）１１、履歴情報１３、及び第２の署名（図１の署名１）１４を、ハードディスク３０４、ＣＤドライブ３０９、ＤＶＤドライブ３１０、またはＦＤＤドライブ３１１などに保存する（ステップＳ２０６）。

【００３７】

次に、図４に示す電子署名を検証する際の処理を説明する。なお、以下では、必要に応じてこの処理を署名検証処理と称する。

なお、電子署名（第１の署名１１及び第２の署名１４）の検証処理を行うときには、第１の署名（図１の署名０）１１、履歴情報１３、及び第２の署名（図１の署名１）１４を、情報処理装置３０１が持っていることを前提とする。ただし、以下の処理も、図２に示す情報処理装置３０１、特に、マウス３１３やキーボード３１４からの入力指示により主記憶装置３０３にロードしたプログラムを、ＭＰＵ３０２などを用いて実行することにより行われる。

【００３８】

まず、原画像１２に対する第１の署名（図１の署名０）１１を確認する（ステップＳ２１１）。これは、原画像１２に対するハッシュ値を生成し、また、第１の署名１１を原画像１２の著作者の公開鍵で変換して出力値を得て、ハッシュ値と出力値とが等しければ、原画像１２が原本であることが保証される。次に、履歴情報１３に対する第２の署名（図１の署名１）１４を確認する（ステップＳ２１２）。これは、履歴情報１３に対するハッシュ値を生成し、また、第２の署名を履歴情報１３の著作者の公開鍵で変換して出力値を得て、ハッシュ値と出力値が等しければ、履歴情報１３が原本であることが保証される。

このように、この２つのデータ（原画像１２と履歴情報１３）の正当性が、電子署名（第１の署名１１と第２の署名１４）により確認された場合には（ステップＳ２１３）、履歴情報１３に書かれている処理と同じ処理を原画像１２に対して行う。これにより、ユーザは、変換処理された画像を得る（ステップＳ２１４）。

【００３９】

一方、ステップＳ２１３において、署名が正しくないと判定された場合には、原画像１２及び履歴情報１３のうちの少なくとも何れか一方は正しくないので処理を中止する。また、このように署名が正しくない場合には、情報（原画像１２、履歴情報１３）に改ざんがあることをユーザに通知するようにしてもよい。

以上のように、本実施の形態では、原画像１２に対する第１の署名（図１の署名０）１１を保持するようにしたので、原画像１２に対する原本性を保証できる。

そして、履歴情報１３に対する第２の署名（図１の署名１）１４を保持するようにしたので、原画像１２の変更処理に対する正当性を保証できる。したがって、原画像１２に対して、著作者が認める正当な変更を行うことができ、画像の最新性を保証できる。

【００４０】

ところで、上述したように、米国特許第５４９９２９４号明細書に記載されている技術では、例えば、デジタルカメラから出力された後に行われた全ての処理は改ざんとして検出される。

そこで、著作者が自分の署名用の秘密鍵を用いて、変更を認めた変更画像に対して電子署名をつけるという解決策が考えられる。しかしながら、この場合、署名した変更画像は独立した画像となり、原画像１２と、原画像１２を変更することにより得られる変更画像との関係が分からなくなるという問題点が残る。さらに、いくつかの変更を著作者が正当と認めた場合、多くの画像と署名のペアを管理する必要があり、メモリ的な制約もでてく

る可能性がある。

これに対して本実施の形態では、第１の署名（図１の署名０）１１及び第２の署名（図１の第２の署名１）１４が正しければ、原画像１２と変更画像との間の関係（処理履歴）を履歴情報１３により知ることができる。

さらに、履歴情報１３は、変更画像に比べてデータ量が少ないので、多くの履歴情報１３を保存しても、それに対応する変更画像をすべて保存することに比べてメモリ容量が小さくなる。これは、後述する第２の実施の形態に示す複数回の変更処理に対して特に有効である。

また、履歴情報１３と署名情報（第１の署名１１、第２の署名１４）は、画像情報に比べて小さいので、原画像１２のヘッダなどに格納することが容易で、多くの履歴情報１３があっても１つのファイルとして管理できる。これも後述する第２の実施の形態に示す複数回の変更処理に対して特に有効である。

【００４１】

（第２の実施の形態）

次に、本発明の第２の実施の形態を説明する。なお、本実施の形態の説明において、第１の実施の形態と同一の部分については同一の符号を付して詳細な説明を省略する。

第１の実施の形態では、１回の処理に対する例を示したが、本実施の形態では、第１の処理の後に、第２の処理、第３の処理・・・と続けて、複数回の処理を正当な処理として認められるようにしている。すなわち、本実施の形態では、以下に示すようにして、原画像１２の原本性を保証しながら、複数回の変更処理による画像の最新性を保証できるようにしている。ここで、第２の処理、第３の処理・・・は、第1の処理と同様に、画像に変更を加える処理である。

【００４２】

ここで、第１の実施の形態の情報処理装置３０１で生成した履歴情報１３を第１の履歴（図５の履歴１）と表す。第１の実施の形態では、図３のフローチャートに従って行われる処理の前提として、原画像１２と第１の署名（図５の署名０）１１は保存されているとしたが、本実施の形態では、２回目の変更に対しては第１の履歴（図５の履歴１）１３と、第１の履歴（図５の履歴１）１３に対する第２の署名（図５の署名１）１４も保存されているとして、図３のフローチャートに従った処理を行う。

【００４３】

その結果、２回目の変更に対する履歴情報として第２の履歴（図５の履歴２）１５と、この第２の履歴１５に対する電子署名である第３の署名（図５の署名２）１６とが生成される。その結果、原画像１２、第１の署名（図５の署名０）１１、第１の履歴（図５の履歴１）１３、及び第２の署名（図５の署名１）１４に加えて、第３の履歴（図５の履歴２）１５と第２の署名（図５の署名２）１６とが保存される。

以下同様にして変更処理を繰り返せば、Ｎ（Ｎは自然数）回の変更処理に対して、原画像１２と、第１～第Ｎの履歴（図５の履歴１～履歴Ｎ）と、第１～第（Ｎ＋１）の署名（図５の署名０～署名Ｎ）とが署名生成処理によって生成され、保存されることになる（図５（ａ）を参照）。

【００４４】

一方、この署名生成処理に対する署名検証処理では、図４のフローチャートにおけるステップＳ２１１の処理、すなわち原画像１２に対する署名確認の処理を行った後に、ステップＳ２１２において、第２の署名（署名１）１３の検証だけでなく、第３～第Ｎ＋１の署名（図５の署名２～署名Ｎ）についても検証を行う。そして、ステップＳ２１３において、これら第２～第（Ｎ＋１）の署名（図５の署名１～署名Ｎ）が正しいと判断された場合には、ステップＳ２１４において、原画像１２に対し、第１～第Ｎの履歴（図５の履歴１～履歴Ｎ）の処理を実行し、原画像１２を変更する。

【００４５】

なお、この場合において、第２～第Ｍ（Ｍは、（Ｎ＋１）より小さい自然数）の署名までは正しく、それ以降の署名が正しくない場合には、全ての処理を中止しなくても第２～

第Ｍの署名に対する第１～第Ｍ－１の履歴の処理を行い、第Ｍ＋１～第Ｎ＋１の署名に対する第Ｍ～第Ｎの履歴の処理を中止することもできる。また、第２～第（Ｎ＋１）の署名（図５の署名１～署名Ｎ）全てを正しいか判定してから、第１～第Ｎの履歴（図５の履歴１～履歴Ｎ）の処理を実行するのではなく、第２の署名が正しければ、第１の履歴の処理を実行し、その後、第３の処理が正しければ、第２の履歴を処理を実行するというように、検証と変更処理を交互に繰り返しても構わない。

【００４６】

以上のように本実施の形態では、１～Ｎ回目の変更に対する履歴情報である第１～第Ｎの履歴と、この第１～第Ｎの履歴に対する電子署名である第２～第（Ｎ＋１）の署名とを生成するようにし、第１～第Ｎの履歴が正しいかどうかを、第２～第（Ｎ＋１）の署名を用いて判断し、正しい場合には第１～第Ｎの履歴に従って原画像１２を変更するようにしたので、１回の変更だけでなく、著作者が正当と認めれば複数回の変更処理を追加しても画像の最新性を常に保証できる。

【００４７】

なお、著作者が、第１の処理を含まない新たな第２の処理も正当と認める場合には、第１の処理の代わりに第２の処理の履歴情報に対して図３と図４に示したフローチャートに従った処理を行えば、第２の処理に対する変更の正当性と原本性とが第１の実施の形態と同様にして保証できることは明らかである。この場合、第１の処理と第２の処理に関する関係は、図５（ｂ）のようになる。このとき、図６に示すようなリスト６０に、履歴情報と電子署名とを処理ごとにまとめて別管理したり、履歴情報のなかにその処理の目的・効果などのアブストラクト的な情報を入れておいたりすることもできる。この履歴情報と電子署名に関する管理は管理データベースを設け、行った変更毎にそのデータベースに登録することによって実現できる。ユーザは必要なときにそのデータベースを参照する。

【００４８】

（第３の実施の形態）

本発明の第３の実施の形態を説明する。なお、本実施の形態の説明において、第１及び第２の実施の形態と同一の部分については同一の符号を付して詳細な説明を省略する。

第１及び第２の実施の形態では、処理の変更はすべて著作者が行う例を示したが、本実施の形態では、多くのユーザが１つのデジタルデータを変更することができるようにする。ここでは、デジタルデータとして電子文書を想定する。そして、図７に示すように、複数のユーザ６０３～６０５がサーバ６０１上で電子文書６０２を共有しており、ネットワーク６００を介して各ユーザ６０３～６０５が電子文書６０２を作成及び変更する場合を想定する。

【００４９】

なお、ユーザ６０３～６０５とは、ユーザが所有する端末のことであり、この端末のハードウェアは、例えば図２に示した情報処理装置３０１により構成されるものである。以下、サーバ６０１及びユーザ６０３～６０５における処理の内容について説明する。

まず、ユーザ６０３が最初のたたき台となる電子文書６０２を作成し、作成した電子文書６０２を第１の文書として、第１の文書に対する署名をつけてサーバ６０１に保存する。なお、以下の説明では、第１の文書に対する署名を第１の署名と称する。また、この第１の署名は、第１及び第２の実施の形態で説明した第１の署名（署名０）１１と同じ方法で作成される。

【００５０】

次に、サーバ６０１に保存された電子文書６０２をユーザ６０４が修正したい場合、ユーザ６０４は、まず、第１の文書と第１の文書に対する第１の署名を確認する。すなわち、第１及び第２の実施の形態と同様に、第１の文書に対するハッシュ値を生成し、また、第１の署名を第１の文書の著作者の公開鍵で変換して出力値を得て、ハッシュ値と出力値とが等しければ、第１の文書が原本であることが保証される。第１の署名が正当であれば、第１の文書に対して修正を施して第２の文書を作成し、第１の文書の修正に関する第１の履歴情報と、この履歴情報に対する第２の署名を付加して保存する。第１の履歴情報と

第２の署名は、それぞれ第１及び第２の実施の形態で説明した第１の履歴情報（履歴１）１３と第２の署名（署名１）１４と同じ方法で作成される。

【００５１】

ここで、全ユーザのアクセス権限が保存されている不図示のアクセス権限データベースに、そのユーザのアクセス権限が設定されている。そして、上記変更処理の正当性の検証は、各ユーザが図２に示すコンピュータへログインする時に得られる認証情報を基に、そのアクセス権限の範囲内の変更であれば正当と判断する一方、その範囲を超えた変更であれば正当でないと判断することによって行うことができる。この他、最初の著作者であるユーザ６０３、もしくは図７のシステムによって、電子文書の内部やヘッダなどにアクセスに関する許諾範囲を設定するようにし、それを、変更処理を行うエディタが読み込んで、許諾範囲内の変更であれば正当と判断する一方、許諾範囲を超えていれば正当でないと判断することによって、上記変更処理の正当性の検証を行ってもよい。

【００５２】

また、上記変更処理の正当性の検証を、公開鍵を用いることによっても行うことが可能である。この場合は、ユーザごとの秘密鍵も用いて署名を生成するのではなく、変更が認められたグループの秘密鍵を用いて署名を生成し、そのグループの公開鍵を用いて、検証を行う。第１の文書に対する第１の署名の正当性を見る際には、このグループの公開鍵を用い、また、第２の履歴情報に対する第２の署名の正当性を見る際にも、先ほど用いたグループの公開鍵を用いて検証することによって、グループ内の誰かが変更処理を行ったことがわかる。

このように、他のユーザまたは同じユーザが文書の修正を繰り返したい場合、修正に関する履歴情報と、この履歴情報に対する署名を付加していくことにより、複数のユーザによる電子文書の管理を実現することができる。

【００５３】

ただし、あるユーザが、それまでの署名を確認したときに、署名が正当でなければその旨を他のユーザに通知する。また、あるユーザが、第１～第Ｍ（Ｍは自然数）の履歴情報までの修正は良いと思うが、それ以降の修正は良くないと思う場合には、良いと思う履歴情報までの修正を行った第Ｍの文書を作成し、そのあと第（Ｍ＋１）の履歴情報とは異なる修正を行う。その後、第Ｍの文書を対象文書として特定する情報（文書番号やハッシュ値など）を履歴情報に入れて、その署名を作成することもできる。この場合、第２の実施の形態で説明した図５（ｂ）のように、作成した署名がそれまでの署名と並列の関係になるので、文書管理システムの中に図６のような署名の関係を示すリスト６０を作成し、分かりやすくすることも可能である。

【００５４】

（第４の実施の形態）

本発明の第４の実施の形態を説明する。なお、本実施の形態の説明において、第１～第３の実施の形態と同一の部分については同一の符号を付して詳細な説明を省略する。本実施の形態では、医療画像に対する医療画像管理システムを例にとり説明する。

システムとしては、図７と同様に、複数のユーザ（医者）６０３～６０５がデジタルレントゲン画像などの電子化された医療画像６０２をネットワーク６００で接続されたサーバ６０１上に共有している場合を想定する。

この場合、医療画像６０２に対する原本性を保証するための情報である第１の署名は、デジタルレントゲン機器に保存されているか、またはデジタルレントゲン機器における医療画像６０２の出力時点で生成され、サーバ６０１に保存されているとする。

【００５５】

まず、医者６０３が医療画像６０２を見る場合、画像内容に関する編集は行わないが輝度変換などの視覚的効果に関する変更を行う。このとき、医者６０３は、毎回その輝度変更を行わないようにするために、原画像である医療画像６０２と変更画像との差分をとり、対象画像を特定する情報や上述したその変更に関するアブストラクト的な情報を、医療画像６０２に付加して第１の履歴情報として保存する。

そして、この第１の履歴情報のハッシュ値に自分の署名を生成し、第２の署名としてサーバ６０１に保存するか、または自分（医者６０３）が所有する端末に保存する。なお、これら第１の履歴情報と第２の署名は、それぞれ第１～第３の実施の形態で説明した第１の履歴情報（履歴１）１３と第２の署名（署名１）１４と同じ方法で作成される。

【００５６】

次に、医者６０４が医療画像６０２を見る場合、その原本性を第１の署名により確認し、他の医者６０３の処理を確認するために第１の履歴情報の正当性を第２の署名により確認し、それを利用またはさらに処理を追加する。

ここで、処理を追加する場合は、第１の履歴情報に従った変更が施された医療画像を変更対象とする場合には、変更対象とする画像に対する情報として第２の署名を第２の履歴情報に含め、さらに、変更対象とする画像と、自分が作成した変更画像との差分画像などを加えて、第３の署名を生成する。また、原画像（医療画像６０２）を変更対象とする場合、第１の署名を第２の履歴情報に含め、さらに、原画像（医療画像６０２）と、自分が作成した変更画像との差分画像などを加えて、第３の署名を生成する。

【００５７】

以下、同様の処理を行うことにより、本実施の形態の医療画像管理システムにおいて、原画像の原本性と変更処理の正当性、及び画像の最新性を同時に実現できる。なお、上記において、第２の履歴情報と第３の署名は、それぞれ第２～第３の実施の形態で説明した第２の履歴情報（履歴２）１５と第３の署名（署名２）１６と同じ方法で作成される。

【００５８】

（第５の実施の形態）

本発明の第５の実施の形態を説明する。なお、本実施の形態の説明において、上述した第１～第４の実施の形態と同一の部分については同一の符号を付して詳細な説明を省略する。本実施の形態では、著作物管理システムを用いたビジネスモデルに関する説明を行う。ここでは、ネットワークに複数のユーザと原画像に対し１次著作権を保有する著作者がある場合を考える。よって、著作者は、図１（ａ）のように、原画像１２とそれに対する第１の署名（署名０）１１を有しているとする。

【００５９】

図８のフローチャートを参照しながら、本実施の形態のシステムにおける処理を説明する。

まず、著作者は、課金などにより正当と認められたユーザに対して、原画像１２を配布する（ステップＳ７０１）。ただし、この原画像１２には、電子透かしなどの著作権保護のための仕組みが入っていても良い。また、この原画像１２には、上述した原本性を示す第１の署名（署名０）１１も添付されている。配布された原画像１２については、ユーザの利用範囲内で変更することが認められているが、原画像１２を含むその変更画像の配布は認められていないとする。

【００６０】

ユーザは、各々、原画像１２の署名を確認した後、著作者から配布された原画像１２に対して、いくつかの変更を試みる（ステップＳ７０２）。ユーザが面白いと思った変更画像を正当な２次著作物としたい場合、ユーザは、著作者に、原画像１２と第１の署名（署名０）１１に加えて自ら行った変更に関する履歴情報である第１の履歴情報１３とその電子署名である第２の署名（署名１）１４を著作者に送る（ステップＳ７０３）。ただし、第２の署名（署名１）１４は、ユーザの秘密鍵で署名されており、それを確認する公開鍵も一緒に送付することができる。

【００６１】

著作者は、第１の署名（署名０）１１と、第２の署名（署名１）１４を確認し、原画像１２に対して第１の履歴情報１３に応じた処理を施す（ステップＳ７０４）。著作者がその処理結果を判定して（ステップＳ７０５）、２次著作物として許諾する場合には、第１の履歴情報１３に対して著作者の秘密鍵による電子署名を生成し、原画像１２と第１の署名（署名０）１１と、第１の履歴情報１３と、第２の署名（署名１）１４と、第３の署名

（署名２）１６とを一緒に保存する（ステップＳ７０６）。一方、許諾しない場合は第３の署名（署名２）１６を生成せずに、その旨をユーザに通知する。

【００６２】

このように、本実施の形態では、原画像１２の著作者が変更処理を認める場合は、変更処理に対する署名を著作者の秘密鍵で生成するので、著作者は、原画像１２である１次著作物から効率的に２次著作物を生成する仕組みを実現することができ、各ユーザは、自分が生成した２次著作物を正当に認められる仕組みを実現することができる。また、このとき、著作者は複数の２次著作物を許可し、その後、著作権料を得ることも可能である。各ユーザは１次著作物を基に容易に２次著作物を生成でき、それによる２次著作権料も得ることができる。さらに、３次著作物以降に対しても全く同様にして適用できる。

【００６３】

（その他の実施の形態）

本発明の目的は、前述した実施形態の機能を実現するソフトウェアのプログラムコードを記録した記録媒体（または記憶媒体）を、システムあるいは装置に供給し、そのシステムあるいは装置のコンピュータ（またはＣＰＵやＭＰＵ）が記録媒体に格納されたプログラムコードを読み出し実行することによっても、達成されることは言うまでもない。この場合、記録媒体から読み出されたプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコードを記録した記録媒体は本発明を構成することになる。

【００６４】

また、コンピュータが読み出したプログラムコードを実行することにより、前述した実施形態の機能が実現されるだけでなく、そのプログラムコードの指示に基づき、コンピュータ上で稼働しているオペレーティングシステム（ＯＳ）などが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

【００６５】

さらに、記録媒体から読み出されたプログラムコードが、コンピュータに挿入された機能拡張カードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれた後、そのプログラムコードの指示に基づき、その機能拡張カードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合も含まれることは言うまでもない。

本発明を上記記録媒体に適用する場合、その記録媒体には、先に説明したフローチャートに対応するプログラムコードが格納されることになる。

【図面の簡単な説明】

【００６６】

【図１】本発明の第１の実施の形態を示し、記録媒体に記録される原画像、署名、及び履歴情報を示した概念図である。

【図２】本発明の第１の実施の形態を示し、情報処理装置の構成の一例を示したブロック図である。

【図３】本発明の第１の実施の形態を示し、電子署名を生成する際の処理を説明するフローチャートである。

【図４】本発明の第１の実施の形態を示し、電子署名を検証する際の処理を説明するフローチャートである。

【図５】本発明の第２の実施の形態を示し、記録媒体に記録される原画像、署名、及び履歴情報を示した概念図である。

【図６】本発明の第２の実施の形態を示し、履歴情報と電子署名とを処理ごとにまとめたリストの一例を示した図である。

【図７】本発明の第３の実施の形態を示し、電子データ管理システムの構成の一例を示したブロック図である。

【図８】本発明の第５の実施の形態を示し、著作物管理システムで行われる処理を説

明するフローチャートである。

【符号の説明】

【００６７】

１１、１４、１６　電子署名

１２　原画像

１３、１５　履歴情報

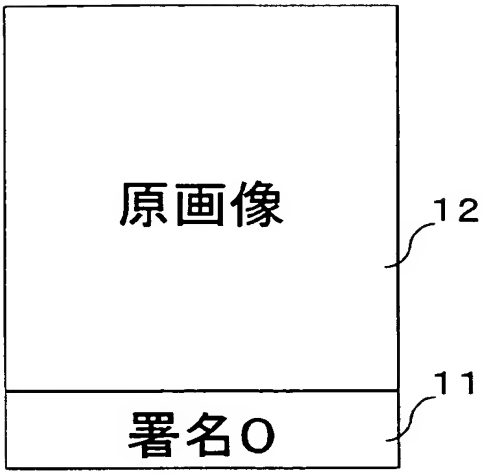
３０１　情報処理装置

６０１　サーバ

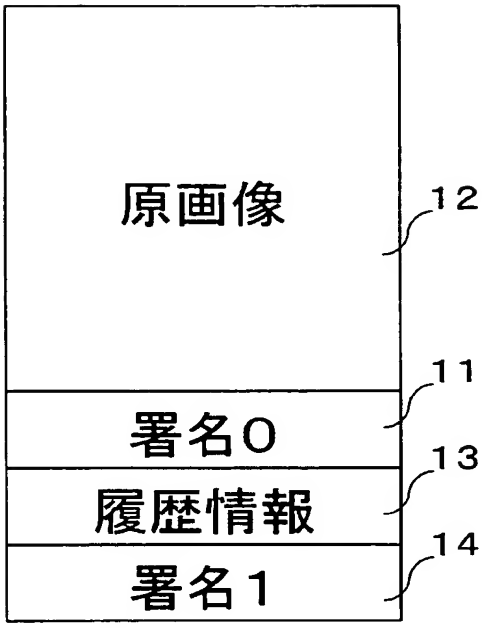
６０２　電子文書

６０３～６０５　ユーザ

【書類名】図面
【図１】

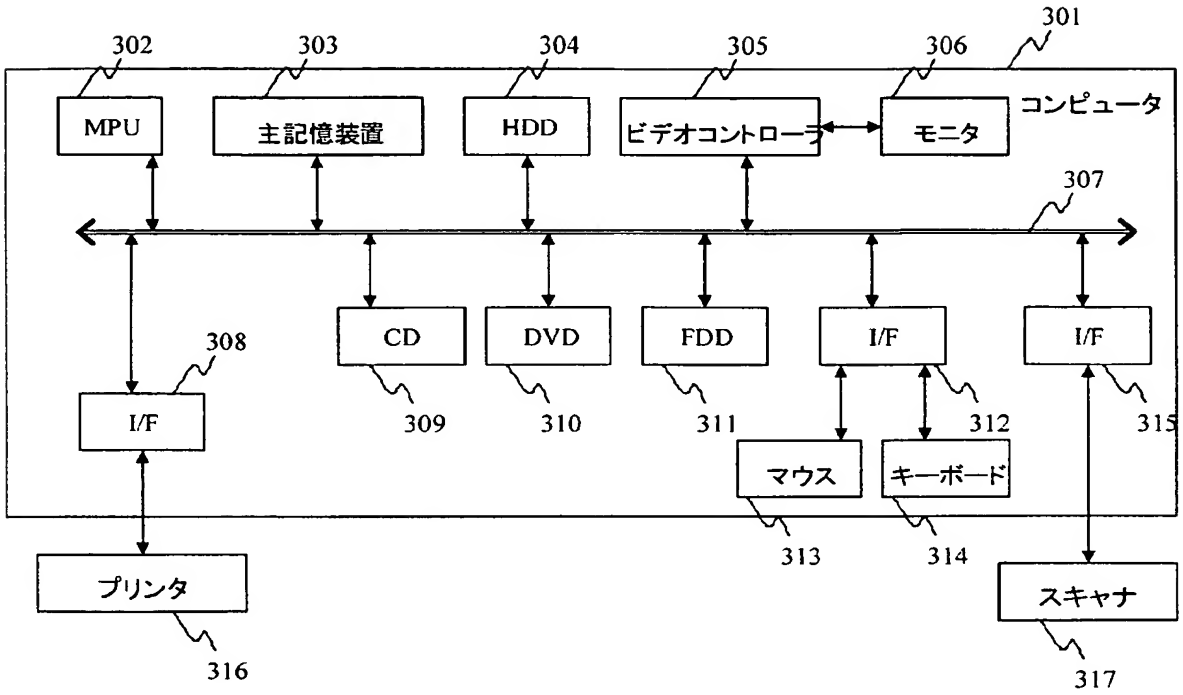


(a)

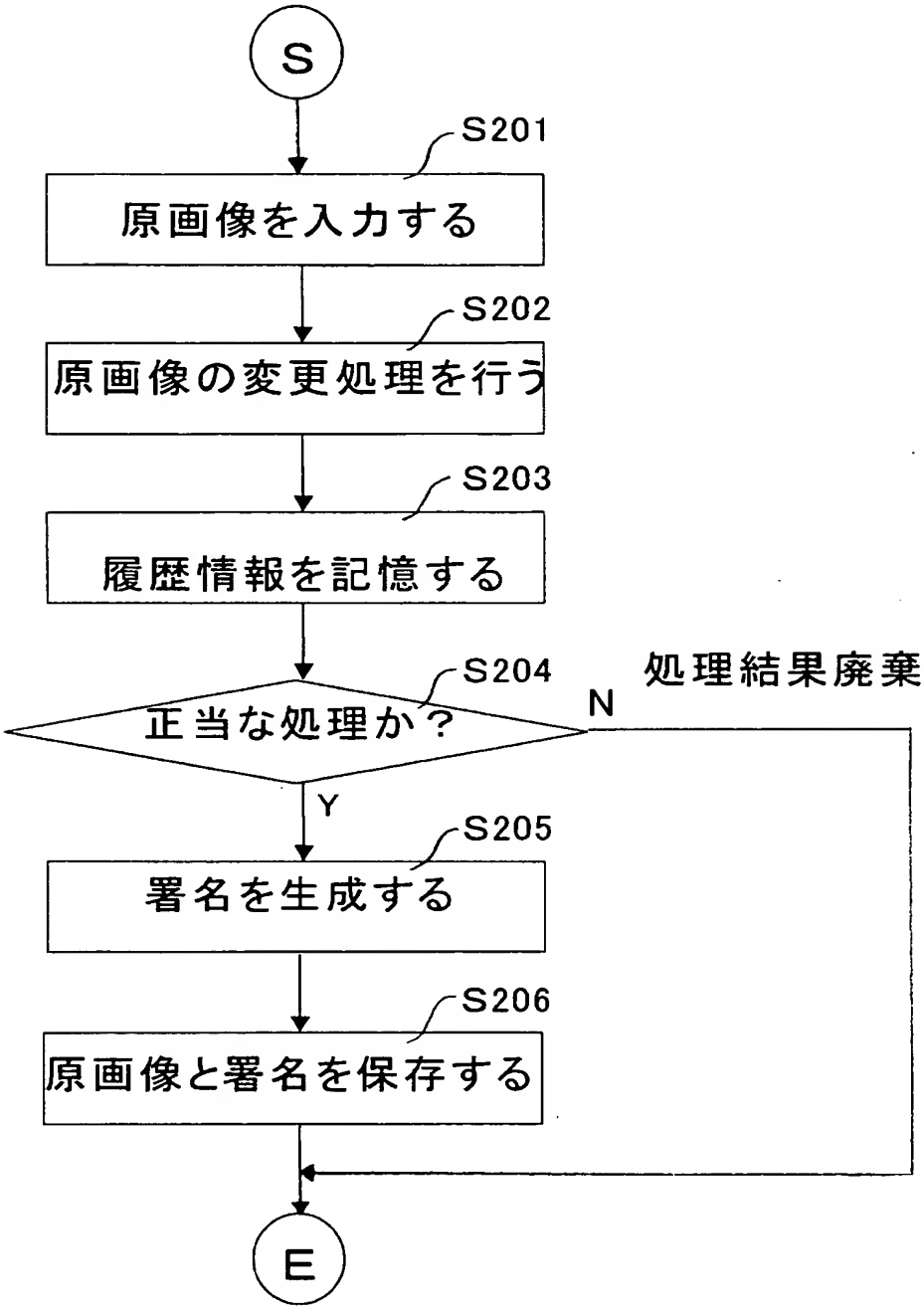


(b)

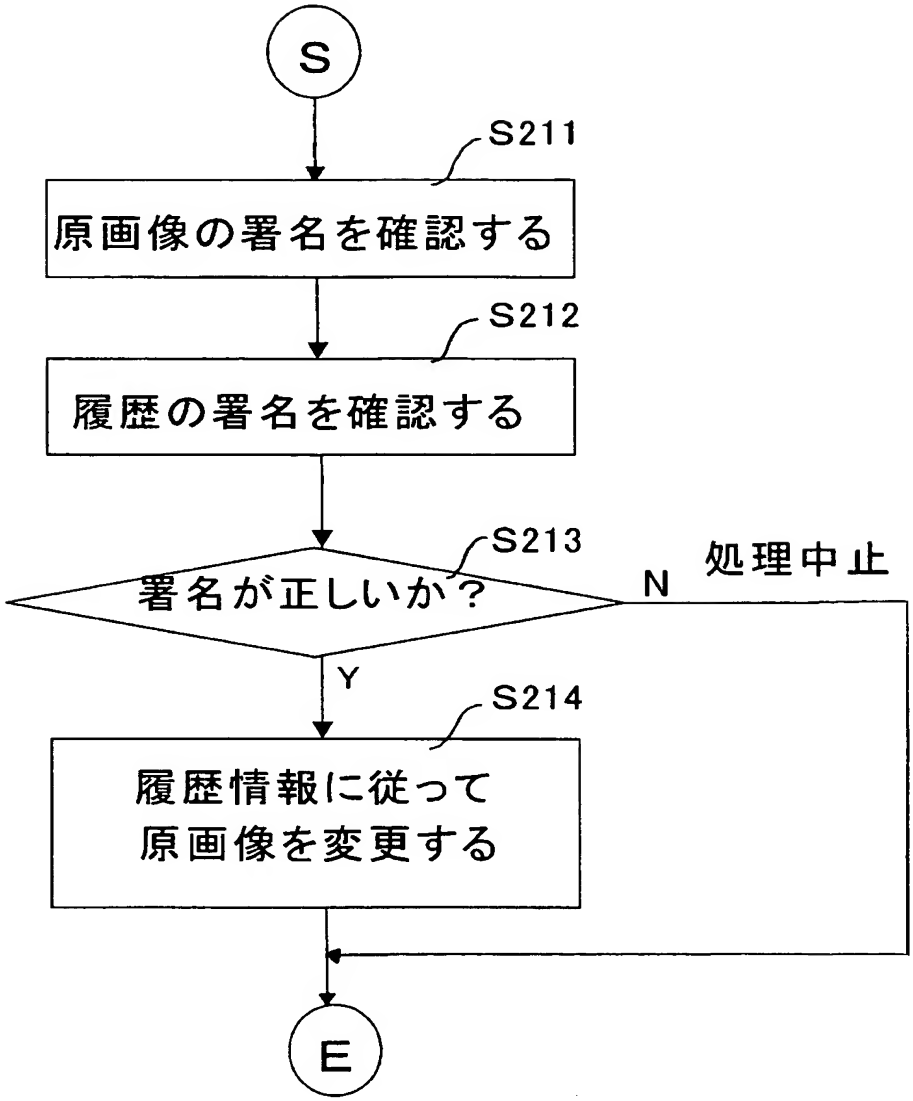
【図２】


301
302
303
304
305
306
MPU
主記憶装置
HDD
ビデオコントローラ
モニタ
コンピュータ
307
308
CD
DVD
FDD
I/F
I/F
I/F
309
310
311
312
315
マウス
キーボード
313
314
プリンタ
スキャナ
316
317

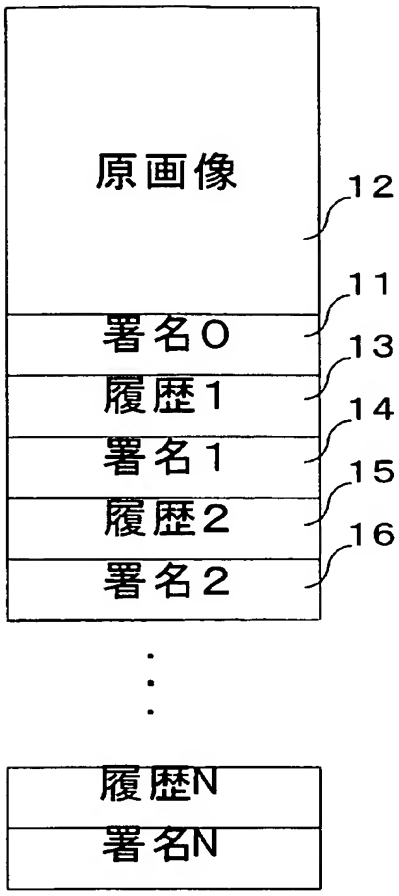
【図３】


S
S201
原画像を入力する
S202
原画像の変更処理を行う
S203
履歴情報を記憶する
S204
正当な処理か？
N
処理結果廃棄
Y
S205
署名を生成する
S206
原画像と署名を保存する
E

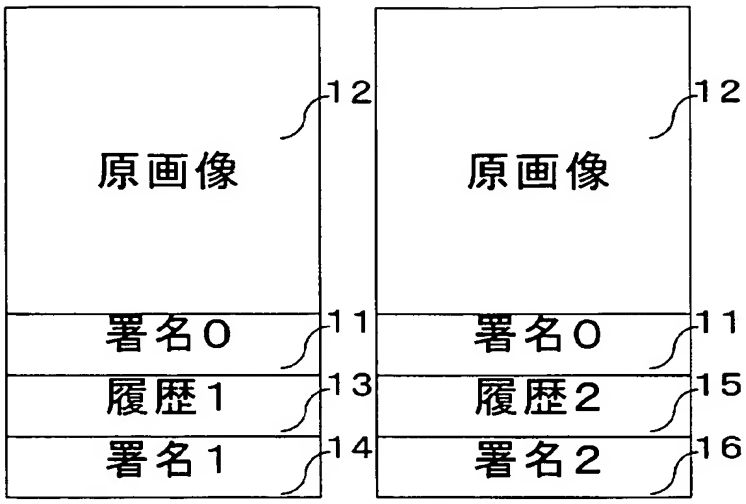
【図４】


S
S211
原画像の署名を確認する
S212
履歴の署名を確認する
S213
署名が正しいか？
N
処理中止
Y
S214
履歴情報に従って
原画像を変更する
E

【図５】


原画像
12
11
署名０
13
履歴１
14
署名１
15
履歴２
16
署名２
履歴N
署名N

(a)


原画像
12
署名０
11
履歴１
13
署名１
14
原画像
12
署名０
11
履歴２
15
署名２
16

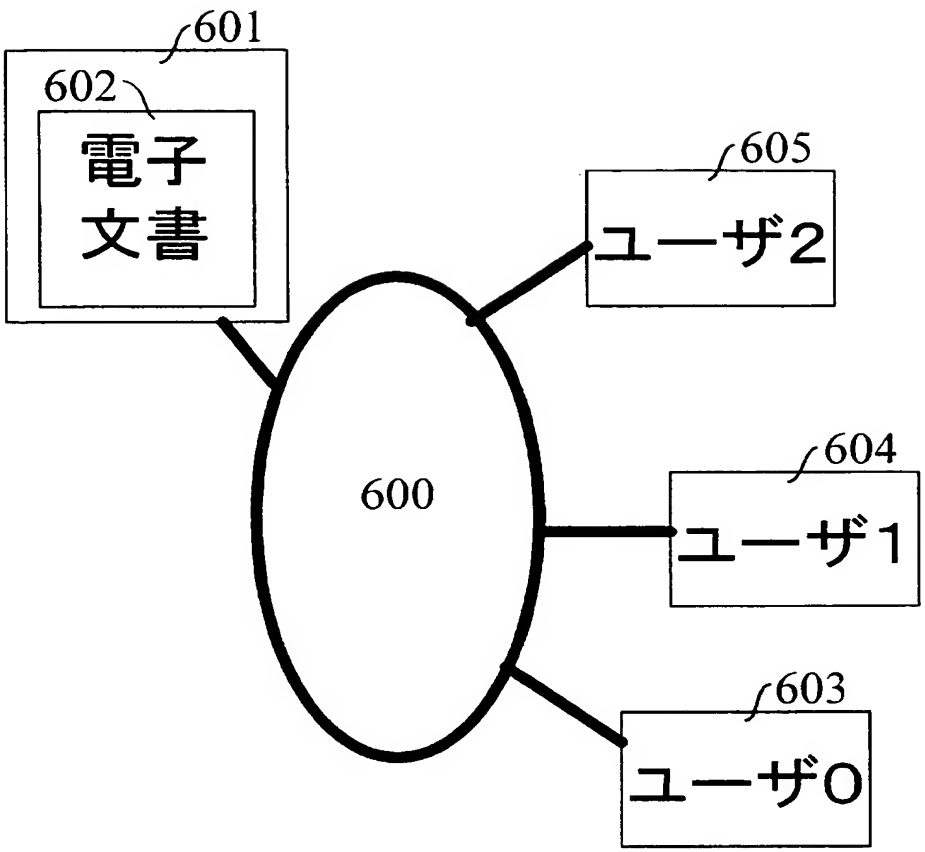
(b)

【図６】

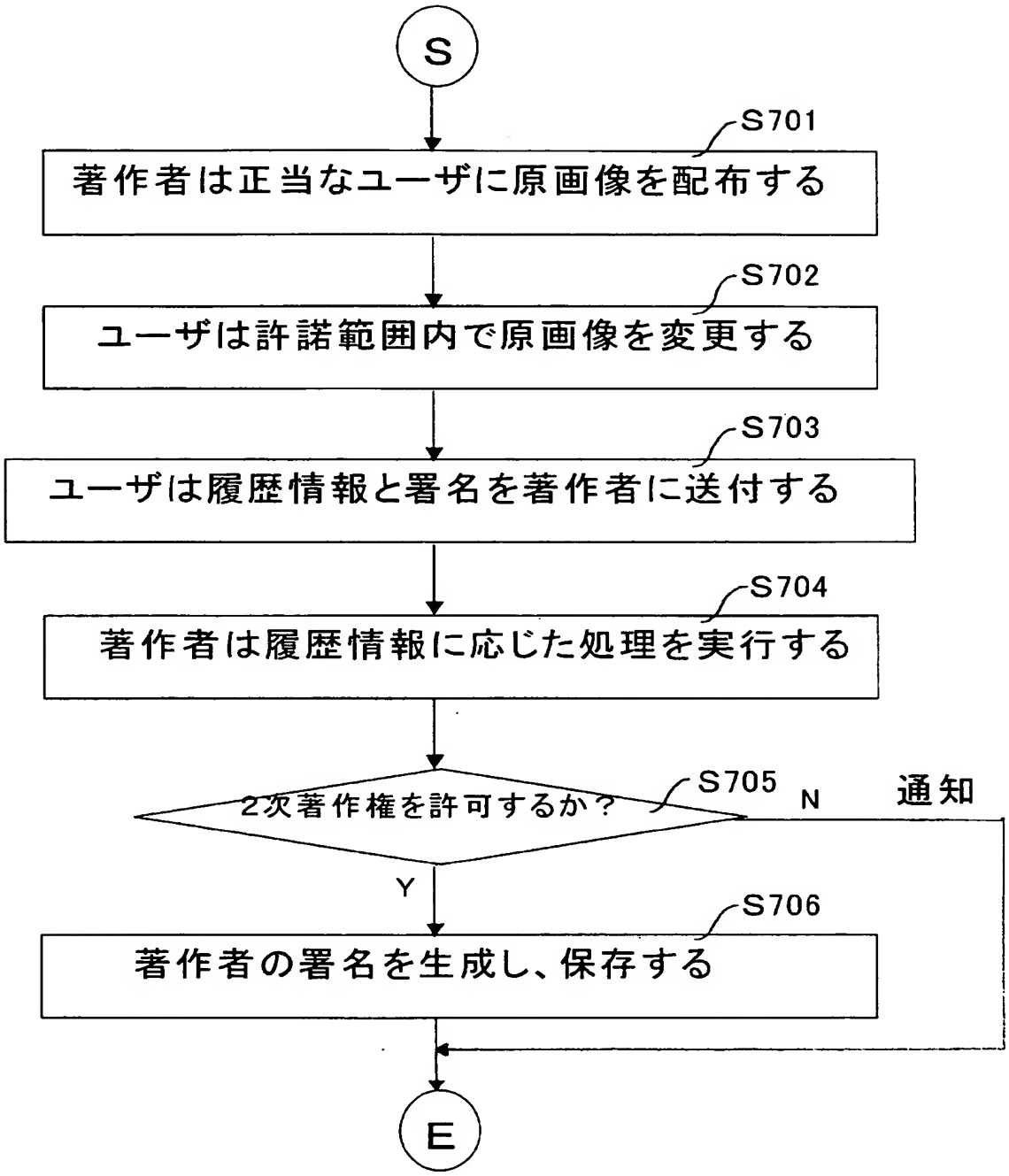
60

履歴情報	電子署名	用途
履歴１	署名１	輝度変換
履歴２	署名２	切り取り
・ ・ ・	・ ・ ・	・ ・ ・

【図７】



【図８】


S
S701
著作者は正当なユーザに原画像を配布する
S702
ユーザは許諾範囲内で原画像を変更する
S703
ユーザは履歴情報と署名を著作者に送付する
S704
著作者は履歴情報に応じた処理を実行する
2次著作権を許可するか？
S705
N
通知
Y
S706
著作者の署名を生成し、保存する
E

【書類名】要約書
【要約】
【課題】　データの原本性を保証しながら、上記データの作者が認める正当な変更を行えるようにする技術を提供することを目的とする。
【解決手段】　所定の作者により作成された原データ（原画像１２）を処理する情報処理装置であって、上記原データを変更する際に、その変更に関する変更情報（履歴情報１３）を記憶媒体に記憶する変更情報記憶部と、上記変更情報が原本であることを保証するための変更保証情報（第２の署名（署名１）１４）を作成する変更保証情報作成部とを有することを特徴とする。
【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－３４６１４０
受付番号	５０３０１６５２５０６
書類名	特許願
担当官	第三担当上席　　００９２
作成日	平成１５年１０月　８日

＜認定情報・付加情報＞

【特許出願人】

【識別番号】　000001007

【住所又は居所】　東京都大田区下丸子３丁目３０番２号

【氏名又は名称】　キヤノン株式会社

【代理人】　申請人

【識別番号】　100090273

【住所又は居所】　東京都豊島区東池袋１丁目１７番８号　池袋ＴＧホーメストビル５階　國分特許事務所

【氏名又は名称】　國分　孝悦

特願２００３－３４６１４０

出　願　人　履　歴　情　報

識別番号　　［０００００１００７］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都大田区下丸子３丁目３０番２号
氏　名　　キヤノン株式会社